Elliptische Kurven als Gruppen

Das Interesse an elliptischen Kurven und auch der Grund für viele ihrer Anwendungen in der Zahlentheorie, Kryptographie und anderen Gebieten beruht wesentlich darauf, daß man die Menge ihrer Punkte in einer natürlichen Weise zu einer Gruppe machen kann. In der Tat kann man zeigen, daß jede (nicht nur ebene) projektive Kurve mit einer durch Polynome gegebenen Gruppenstruktur bijektiv in eine elliptische Kurve übergeführt werden kann.

Zur Definition einer Gruppenoperation müssen wir einem Paar aus zwei Punkten einen dritten Punkt zuordnen. Da wir elliptische Kurven als ebene Kurven vom Grad drei definiert haben, können wir dazu die Tatsache ausnutzen, daß nach dem Satz von BÉZOUT jede Gerade mit Vielfachheiten gezählt eine kubische Kurve in genau drei Punkten schneidet – zumindest wenn der Grundkörper algebraisch abgeschlossen ist.

Wenn wir für eine elliptische Kurve E über einem beliebigen Körper k die Gerade durch zwei Punkte $P, Q \in E$ betrachten, hat die Gleichung dieser Geraden Koeffizienten aus k. Wenn wir sie in die Kurvengleichung einsetzen, erhalten wir eine kubische Gleichung für eine der Koordinaten der drei Schnittpunkte; da zwei davon Koordinaten in k haben, muß das auch für den dritten gelten.

Wir könnten also versuchen, eine Verknüpfung zu definieren, indem wir zwei Punkten P, Q den dritten Schnittpunkt R der Geraden durch P und Q zuordnen.

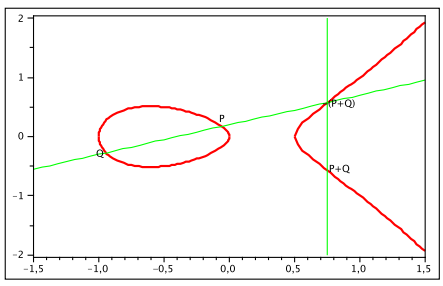
Leider führt dieser Ansatz aber nicht zu einer Gruppenverknüpfung: Wenn wir eine Gruppe hätten, gäbe es ein Neutralelement $O \in E$, dessen Verknüpfung mit jedem Punkt P gleich P sein müßte, d.h. der „dritte“ Schnittpunkt der Geraden durch P und O wäre P, so daß die Gerade OP die Kurve E in P mit Vielfachheit zwei schneiden müßte. Für jeden Punkt $P \in E$ wäre also die Gerade durch O und P die Tangente an E im Punkt P. Damit müßten also alle Tangenten an E durch einen einzigen Punkt $O \in E$ gehen! Damit wäre dann auch für jeden Punkt $P \in E$ die Summe $P + P = O$, d.h. jedes Element $P \in E$ hätte die Ordnung zwei.

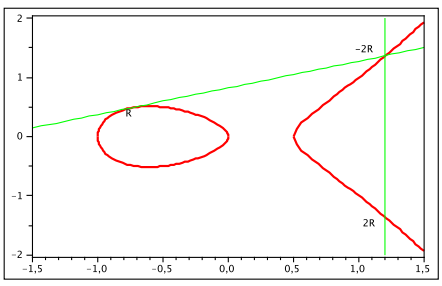
Für eine Gerade gehen natürlich alle Tangenten durch einen (und nicht nur einen) Punkt, denn hier sind sogar alle Tangenten gleich der Geraden. Für Kurven höheren Grades fällt es aber schwer, sich so etwas vorzustellen, und in der Tat bewies PIERRE SAMUEL 1966, daß die einzigen Beispiele solcher Kurven Quadriken (also Kurven vom Grad zwei) über Körpern der Charakteristik zwei sind; siehe

> PIERRE SAMUEL: Lectures on old an new results on algebraic curves, *Tata Institute of Fundamental Research Lectures on Mathematics and Physics* **36**, Bombay, 1966

Für die Parabel mit der affinen Gleichung $y = x^2$ beispielsweise verschwindet $y' = 2x$ überall, da $2 = 0$ ist. Daher sind alle Tangenten parallel zur x-Achse und gehen somit alle durch deren unendlichfernen Punkt $(1 : 0 : 0)$. Dieser Punkt liegt aber natürlich nicht auf der Kurve, denn bei einer irreduziblen Kurve vom Grad zwei kann die Tangente an einen Kurvenpunkt nach BÉZOUT keinen weiteren Schnittpunkt mit der Kurve haben. In der Tat erfüllt $(1 : 0 : 0)$ nicht die homogenisierte Gleichung $yz = x^2$.

Eine leichte Modifikation führt aber zu einer Gruppenstruktur: Wenn drei Punkte P, Q und R von E auf einer Geraden liegen, soll das nicht bedeuten, daß $R = P + Q$ ist, sondern daß $P + Q + R$ gleich dem Neutralelement O ist; somit ist also $R = -(P + Q)$. Die beiden Abbildungen zeigen dies für den Fall, daß O – wie bei WEIERSTRASS-Gleichungen üblich – der unendlichferne Punkt $(0 : 1 : 0)$ der y-Achse ist. Das Inverse eines Punktes $P \in E$ ist dann einfach der zweite Schnittpunkt der Geraden parallel zur y-Achse durch P mit E, denn natürlich muß in jeder Gruppe $P + O + (-P) = P + (-P) = O$ sein.





Was uns noch fehlt zur Definition der Verknüpfung ist die Wahl eines geeigneten Punktes O. In einer Gruppe muß natürlich $O + O = O$ und

damit auch $O+O+O=O$ sein, d.h. die Tangente im Punkt O schneidet mit Vielfachheit drei, so daß O ein Wendepunkt sein muß.

Wie wir in der Vorlesung über die WEIERSTRASSsche Normalform gesehen haben, ist jede elliptische Kurve zumindest über einem Körper, dessen Charakteristik von zwei und drei verschieden ist, birational äquivalent zu einer Kurve mit einer WEIERSTRASS-Gleichung, und diese hat den Punkt $(0:1:0)$ als Wendepunkt. Wir werden uns daher beschränken auf elliptische Kurven mit mindestens einem Wendepunkt, und wählen für O einen der Wendepunkte.

Damit definieren wir die Inversenabbildung $E \to E$ dadurch, daß ein Punkt $P \in E$ abgebildet wird auf den dritten Schnittpunkt $-P$ der Geraden durch O und P mit E.

Die Gruppenverknüpfung $E \times E \to E$ definieren wir dadurch, daß wir für ein Punktepaar (P,Q) den dritten Schnittpunkt R der Geraden durch P und Q mit E bestimmen und $P+Q=-R$ setzen.

Satz: Mit der so definierten Verknüpfung und Inversenabbildung wird E zu einer abelschen Gruppe mit Neutralelement O.

Beweis: Das Kommutativgesetz ist klar, denn die Gerade durch P und Q ist natürlich gleich der Geraden durch Q und P, und damit ist auch der dritte Schnittpunkt R in beiden Fällen der gleiche.

Auch mit den inversen Elementen gibt es keine Probleme, denn $-P$ ist gerade so definiert, daß die Gerade durch P und $-P$ den Punkt O als dritten Schnittpunkt hat. Somit ist $P+(-P)=-O$, und da O ist Wendepunkt ist, muß $-O=O$ sein.

O ist tatsächlich das Neutralelement, denn für jeden Punkt $P \in E$ hat die Gerade durch O und P den Punkt $-P$ als dritten Schnittpunkt mit E, so daß $P+O=O+P=-(-P)$ ist, und aus der Definition der Inversenabbildung folgt sofort $-(-P)=P$.

Bleibt noch das Assoziativgesetz. Bei den meisten bekannten Gruppen ist dieses recht einfach nachzurechnen; hier ist das leider nicht der Fall. In der Tat brauchen wir die meisten der allgemeinen Resultate über projektive ebene Kurve vor allem dazu, um dieses Gesetz nachzuweisen.

Seien also $P, Q, R \in E$ drei Punkte der Kurve; wir müssen zeigen, daß

$$(P + Q) + R = P + (Q + R)$$

ist. Mit den Abkürzungen $P + Q = S$, $S + R = T$ und $Q + R = U$ wird es zu $T = P + U$; wir müssen also zeigen, daß die drei Punkte P, U und $-T$ auf einer Geraden liegen.

Dazu betrachten wir zunächst die Geraden, die zur Berechnung der Summen und Inversen benötigt werden:

Die Gerade g_1 durch P und Q hat $-S$ als dritten Schnittpunkt mit E.

Die Gerade g_2 durch S und R hat $-T$ als dritten Schnittpunkt mit E.

Die Gerade g_3 durch O und U hat $-U$ als dritten Schnittpunkt mit E.

Die Gerade h_1 durch S und O hat $-S$ als dritten Schnittpunkt mit E.

Die Gerade h_2 durch Q und R hat $-U$ als dritten Schnittpunkt mit E.

Die Vereinigung $C = g_1 \cup g_2 \cup g_3$ der drei ersten Geraden ist eine (reduzible) kubische Kurve, die mit der irreduziblen Kurve E keine Komponente gemeinsam hat. Nach dem Satz von BÉZOUT gibt es daher mit Vielfachheiten gezählt über einem algebraisch abgeschlossenen Körper, der k enthält, genau neun Schnittpunkte. Da die neun Punkte $O, P, Q, R, S, -S, -T, U$ und $-U$ allesamt sowohl auf E als auch auf C liegen, sind dies alle Schnittpunkte. Sechs davon, nämlich $O, R, S, -S, Q$ und $-U$, liegen auch auf der (reduziblen) Quadrik $h_1 \cup h_2$.

Als wir Schnittpunkte ebener kubischer Kurven betrachteten, haben wir unter anderem folgendes bewiesen: Wenn zwei ebene kubische Kurven ohne gemeinsame Komponente neun Schnittpunkte haben, von denen sechs auf einer Quadrik liegen, liegen die restlichen drei auf einer Geraden.

Dies wenden wir an auf die kubischen Kurven E und C sowie die Quadrik $h_1 \cup h_2$: Die restlichen drei Schnittpunkte P, U und $-T$ müssen demnach auf einer Geraden liegen, und das ist nach unserer Definition der Addition äquivalent dazu, daß $P + U = T$ ist. Damit ist auch das Assoziativgesetz und damit der ganze Satz bewiesen.

■

Als erstes Beispiel dafür, wie die Gruppenstruktur mit der Geometrie zusammenhängt, wollen wir die Wendepunkte einer elliptischen Kurve betrachten.

Wir gehen also aus von einer elliptischen Kurve E über einem Körper k, die mindestens einen Wendepunkt hat. (Andernfalls funktioniert unsere Definition der Gruppenverknüpfung nicht, und wir bräuchten etwas komplizierteres.)

Geometrisch können wir die Wendepunkte bestimmen als die Schnittpunkte von E mit ihrer HESSEschen Kurve H. Auch diese ist eine kubische Kurve; damit gibt es nach dem Satz vonBÉZOUT über einem algebraisch abgeschlossenen Körper K, der k enthält, mit Vielfachheiten gezählt genau neun Schnittpunkte. Wie wir bereits wissen, ist die Vielfachheit eines Schnittpunkts gleich der Vielfachheit des Wendepunkts; da die Wendetangente im Falle einer kubischen Kurve nicht mit einer größeren Vielfachheit als drei schneiden kann, sind hier alle Wendepunkte und damit auch alle Schnittpunkte einfach. Somit gibt es genau neun Stück in $E(K)$.

Für einen Wendepunkt $P \in E$ schneidet die Wendetangente im Punkt P mit Vielfachheit drei, d.h. $P+P = (-P)$ und damit $P+P+P = 3P = O$. Die Wendepunkte sind also genau die Punkte $P \in E$ mit $3P = O$. Diese Punkte bilden offensichtlich eine Untergruppe, denn ist $3P = 3Q = O$, so ist auch $3(P+Q) = 3P+3Q = O$; außerdem ist $3(-P) = -3P = O$, und natürlich ist auch $3O = O$.

Wenn wir anstelle von E die Kurve $E(K)$ betrachten, haben wir dort natürlich auch eine Gruppenstruktur, und $E = E(k)$ ist eine Untergruppe von $E(K)$. In $E(K)$ bilden die Wendepunkte eine Untergruppe mit neun Elementen; die Wendepunkte in $E = E(k)$ sind eine Untergruppe davon. Nach einem Satz von LAGRANGE ist die Ordnung (Elementanzahl) einer Untergruppe ein Teiler der Gruppenordnung; es gibt daher entweder einen oder drei oder neun Wendepunkte.

Die Gerade durch zwei Wendepunkte P und Q schneidet die Kurve außerdem noch im Punkt $-(P+Q)$; da natürlich auch $3\big(-(P+Q)\big) = O$ ist, schneidet die Gerade durch zwei Wendepunkte die Kurve also wieder in einem Wendepunkt.

Falls es nur einen Wendepunkt gibt, ist das der Punkt O; die Gerade durch O und O ist die Wendetangente, die natürlich O als „dritten“ Schnittpunkt hat, denn sie schneidet mit Vielfachheit drei.

Falls es drei Wendepunkte gibt, folgt, daß sie auf einer Geraden liegen müssen.

Falls es neun Wendepunkte gibt, liegt auf der Geraden durch zwei verschiedene Wendepunkte stets noch ein weiterer Wendepunkt. Es gibt $\binom{9}{2} = \frac{1}{2} \cdot 9 \cdot 8 = 36$ Paare verschiedener Wendepunkte; jede Gerade, auf der drei Wendepunkte liegen, läßt sich durch drei solche Paare charakterisieren. Somit gibt es zwölf Geraden, die die Kurve in jeweils drei Wendepunkten schneiden, und jeder Wendepunkt liegt auf vier dieser Geraden.

Man kann dies auch ohne Verwendung der Gruppenstruktur beweisen, indem man die Schnittmenge von E und H genau analysiert; allerdings ist das erheblich aufwendiger und umständlicher.